UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Crim. No. 11-CR-10260-NMG
	)	
AARON SWARTZ,	)	
Defendant	)	

DEFENDANT AARON SWARTZ'S SUPPLEMENTAL SUBMISSION IN SUPPORT OF HIS MOTION TO COMPEL DISCOVERY AND A PROTECTIVE ORDER

Aaron Swartz provides this supplemental submission to address certain issues raised during the October 11, 2011 hearing. The Court identified two categories of discoverable data:

(1) the data allegedly downloaded from JSTOR's website; and

(2) nine email chains of communications between MIT and JSTOR about the downloading and vulnerabilities that allegedly enabled or might enable downloading to occur.

I. THE DOWNLOADED DATA.

A. Security Arrangements.

Both in its motion seeking a protective order and at the hearing, the government attempts to justify an order that the defense be required to use the downloaded data to litigate this case and prepare for trial solely in a Secret Service office. Its insistence on keeping the data solely in the government's possession is based on a claim that "The government can secure this data to an extent that a law office cannot." Motion of the United States for a Protective Order, Dkt 18, at 3. The government claims that it is primarily concerned with preventing third parties from obtaining access to the

downloaded data. *Id*. It agrees that the defense counsel and its experts and investigators can be trusted to use the data lawfully. It has presented no evidence that Mr. Swartz cannot be similarly trusted to use the information exclusively for the defense of this case. Neither the government nor the Court can deny that Mr. Swartz is the most important member of the defense team who must examine and analyze discoverable data, including the downloaded data.

The government cannot and does not deny that the defense's searches and other work with the downloaded data is privileged information. The defense's selection of searches and other examinations of the downloaded data would be recorded in electronic data that would remain in the government's possession. For that reason, if its proposed protective order is approved by the Court, the government would have impermissible and unconstitutional access to the defense's work product-protected data. *See United States v. Horn*, 29 F.3d 754, 757-758 (1st Cir. 1994)(government surveillance of defense's selections from discoverable documents constitutes prosecutorial conduct).

The defense proposes that the downloaded data be provided to it at the offices of Collora LLP, which is on the 12th floor of the Federal Reserve Bank Building in Boston. That building and office is at least as secure as any other government building and office in Boston, including the US Attorney's office and the Secret Service office. The downloaded data would be stored in a locked space within the Collora LLP office suite. The keys would be possessed exclusively by undersigned counsel and William Kettlewell, a Collora LLP partner who was a consultant on the defense team prior to the indictment who met with the government and undersigned counsel prior to the indictment, and remains a member of the defense team without having filed his

appearance. Mr. Kettlewell is willing to sign a protective order, as are the defendant and all members of the defense team. The data would be stored and accessible only on an off-line computer at Collora LLP that is not connected to the Internet. In the event that the defense contends that it is necessary to modify the restrictions on storage, access and use of the downloaded data, the defense would be required to seek court approval. Terms for such a protective order are attached hereto as Exhibit 1.

B. Severance of Metadata From Articles and Other Text.

At the hearing, the Court ordered the government to inform the Court whether it is feasible to sever the metadata from the articles to which the metadata relates. The government has informed the defense counsel that it proposes to provide the defense with the metadata without the pdf files to which the metadata relates. The defense is entitled to, and must have, the same full set of downloaded data, including the pdf files that the government has, in order to litigate this case through a trial. Without the articles and other pdf files, the defense cannot effectively and efficiently conduct its analysis of exactly what was downloaded from where and under what circumstances. The metadata alone does not provide this essential set of full information. In view of the security arrangements proposed by the defense, there is no justification for redacting discoverable data and subjecting the defense to an unconstitutional burden of having to seek essential information about the downloaded data from the government. These defense requests would, in turn, disclose work product privileged information. The defense cannot be required to conduct this litigation without information that Rule 16 entitles it to have in order to provide even-handed access to evidence and information.

II. THE NON-DOWNLOADED DATA.

The government proposes that Mr. Swartz be prohibited from receiving copies of nine email chains. Instead, it proposes that Mr. Swartz read, and work at his counsel's office with, these nine email chains pertaining to "security weaknesses" of MIT's and JSTOR's computer networks. Mr. Swartz is willing to sign a protective order restricting his use of this information to the litigation of this case. That is all that is necessary to provide a more than sufficient assurance against any improper or unlawful use of copies of these email chains.

The defense team, including Mr. Swartz, his lawyers, investigators and experts, are located in several cities, only one of which is Boston. Communication of privileged information within the defense camp occurs by password-protected, confidential email. Arguendo, even if the government's mistrust of Mr. Swartz is taken at face value, its proposal does not afford any substantial security against improper use of this discoverable information. Mr. Swartz must and will have all of the information in these nine email chains. These emails about means of access to MIT and JSTOR networks, characterized by the government as "vulnerabilities," may contain important exculpatory information, or may lead to exculpatory evidence. There is no basis in this record for Mr. Swartz to be the only member of the defense team who can have this information, but cannot have copies, to use for his defense.

Mr. Swartz must be able to make notes and send memoranda to the defense team about these nine emails after studying them up to and including the trial. He is not usually in Boston during the work week. He must work on this case on nights and

weekends. As to these nine email chains, the defense would transmit them as password-protected documents sent by electronic mail. The defense is willing to password protect these particular discovery materials by circulating them electronically among members of the defense team as provided in Exhibit1.

In any event, based on this record, this Court should view with skepticism the government's unsupported claim that disclosure of the nine email chains threatens harm to either MIT or JSTOR. There is no affidavit or evidence in any form to support that claim. JSTOR's counsel did not express concern about any non-downloaded data including its communications with MIT or anyone else. MIT has not objected to disclosure of this supposedly sensitive information either. Even if MIT or JSTOR objected to disclosure, these documents are putative evidence that the defense may be entitled to admit during Mr. Swartz's public trial. Because these documents are potential evidence in a public trial, refusing to make copies available to Mr. Swartz cannot be justified. The government has abandoned its claim that Mr. Swartz cannot be trusted to have a copy of three lines of code he allegedly wrote and used to download data. It has unjustifiably withheld huge amounts of discoverable data for weeks by making wildly unsupported security claims that it has now abandoned. Mr. Swartz should have copies of the nine email chains exclusively for his use in defending this case.

III. THE SEIZED DATA, DEFENDANT'S STATEMENTS, AND EXCULPATORY EVIDENCE

The Court should order the government to provide copies of the following:

1. **Defendant's Written Statements.** The defendant's written statements that are within its custody, possession and control, e.g., Twitter and Facebook postings,

websites, text messages and electronic mail. The government obtained some of this information as the fruit of warrantless seizures of devices that the government asserts belong to Mr. Swartz; some are the fruit of warrant-authorized seizures of items that the government asserts belong to Mr. Swartz; and some information was obtained in response to grand jury subpoenas to electronic communications providers. The defendant's written statements are subject to automatic discovery. Local Rule 116.1(C)(1)(a) and Rule 16(a)(E). In paragraph A.1.a. of its August 12, 2011 letter to defense counsel (attached hereto as Exhibit 2), the government states that it will offer some of these written statements in its case-in-chief. The defendant's written statements are also material to the defense. The government does not provide any "good cause" for withholding the defendant's written statements.

2. **Seized Electronic Data.** In its August 12, 2001 letter, the government listed the items containing electronic data stored in electronic data storage media that it has seized as follows:

- Acer laptop computer recovered at MIT
- Western Digital hard drive recovered at MIT*
- HP USB drive seized from the defendant at the time of his arrest
- Apple iMac computer seized at Harvard
- Western Digital hard drive seized at Harvard
- HTC G2 cell phone seized during the search of the defendant's residence
- Nokia 2320 cell phone seized during the search of the defendant's residence
- Sony Micro Vault seized during the search of the defendant's residence

The government has no good cause to withhold copies of the seized electronic data, all of which is discoverable under Rule 16(a)(1)(E). For that reason, the

* Search warrant applications for devices seized at MIT and Harvard allege probable cause to believe that these devices belong to Mr. Swartz and are evidence of the commission of the offenses charged in the indictment.

instant motion seeks an order compelling the government to provide the defense with copies in the form of bit-by-bit, mirror electronic images of all of the data natively stored on the above-listed electronic devices, including any and all metadata. In order to effectively defend himself against the indictment's allegations, Mr. Swartz is constitutionally entitled to an exact and complete copy of the discoverable electronically stored information in its native format so that he may examine and, if appropriate, contest the provenance and substance of that evidence. *See United States v. Briggs, 2011 U.S. Dist. LEXIS 101415 (W.D.N.Y.).*

3. **Complete Video Recordings.** Paragraph E of the government's August 12, 2011 letter states that it has provided copies of what it considers to be the "relevant portions" of video recordings made on January 4 and 6, 2011, in a wiring closet in the basement of MIT's Building 16. Under Rule 16, Mr. Swartz is entitled to full and complete copies of all video recordings made in that closet including but not limited to recordings made at any time including, but not limited to, January 4 and 6, 2011, because the complete records contain evidence that is material to his defense.

4. **Exculpatory Evidence**. In paragraph H of the government's letter, the government described but refused to provide almost all of certain exculpatory evidence, including evidence that, during the period covered by the indictment, persons other than Mr. Swartz at Harvard, MIT and China accessed the Acer laptop that was seized by the government, and persons other than Mr. Swartz at MIT and elsewhere were engaging in "journal spidering" of JSTOR data using a "virtual computer" that can be hosted by anyone at MIT. The government has no

basis for withholding the electronic evidence described as exculpatory in its letter.

CONCLUSION.

For all the foregoing reasons, the Court should enter the order attached hereto as Exhibit 1.

Respectfully submitted,

/s/Andrew Good
Andrew Good
BBO # 201240
Good & Cormier
83 Atlantic Avenue
Boston, MA 02110
Tel. 617-523-5933
agood@goodcormier.com

CERTIFICATE OF SERVICE

I hereby certify that the foregoing document filed through the ECF system will be sent to counsel for the government who are registered participants as identified on the Notice of Electronic Filing ("NEF").

DATED: October 24, 2011

/s/ *Andrew Good*
Andrew Good

G:\CLIENTS\Swartz, Aaron\Pleadings - Federal Court Case\Supplemental Submission in Support of Motion to Compel.doc

Exhibit 1

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Crim. No. 11-CR-10260-NMG
	)	
AARON SWARTZ,	)	
Defendant	)	

(PROPOSED) ORDER

After consideration of the Government's motion for a protective order, the Defendant's motion to compel discovery, and the oppositions filed by both parties in response to the motions, it is ordered that the Government shall provide copies, or enable the Defendant to make copies, of the following that are within its possession, custody or control:

1. All electronic data that constitutes or includes a written statement of Mr. Swartz including communications on Twitter, Facebook, text message and email or any other form of electronic communication.
2. All data, documents, and tangible things including, but not limited to, data obtained from MIT and JSTOR, that are discoverable under Rule 16(a)(1)(E). All data includes: (A) all data seized from devices that the government has asserted belong to the defendant, including:

    - Acer laptop computer recovered at MIT
    - Four Samsung hard drives delivered to the Secret Service by Defendant Swartz and his counsel on June 7, 2011
    - Western Digital hard drive recovered at MIT*
    - HP USB drive seized from the defendant at the time of his arrest
    - Apple iMac computer seized at Harvard

* Search warrant applications for devices seized at MIT and Harvard allege probable cause to believe that these devices belong to Mr. Swartz and are evidence of the commission of the offenses charged in the indictment.

- Western Digital hard drive seized at Harvard
- HTC G2 cell phone seized during the search of the defendant's residence
- Nokia 2320 cell phone seized during the search of the defendant's residence
- Sony Micro Vault seized during the search of the defendant's residence

(B) All data and items that are material to preparing the defense, namely, all data and items that constitute, or are evidence of, the occurrences and activity, including electronic communications, transmissions, and activity, that the government alleges occurred in the indictment.

(C) All data and items that the government intends to use in its case-in-chief.

(D) With respect in particular to any and all data that the government alleges was illegally downloaded from JSTOR's database including, but not limited to the data stored in the Four Samsung hard drives delivered to the Secret Service by Defendant Swartz and his counsel on June 7, 2011 ("the downloaded data"), the government shall provide one bit by bit copy of the downloaded data in its native format to the defense at the office of Collora LLP, 400 Atlantic Avenue, Boston, into the custody of Attorney William Kettlewell who shall sign a copy of this order. Access to the room in which the downloaded data shall be stored at Collora LLP shall be controlled by keys to be kept in the sole custody of Mr. Kettlewell and Andrew Good. The downloaded data in the custody of Mr. Kettlewell and Mr. Good shall be accessed solely on an offline computer that is not connected to the internet. Until and unless this Court approves a written modification of this order, each member of the defense, including Mr. Swartz, may have access to the

downloaded data in the offices of Collora LLP, and at no other location, and only after signing a copy of this order.

(E) In the event that the defense electronically transmits copies of any or all of the nine email chains designated by the government by means of any form of internet communication including email, access to copies of any of the nine email chains must be protected by a privileged password.

3. All data, documents, and tangible things that constitute or are evidence of the potentially exculpatory information described in paragraph H.1 and H.5 of the government's August 12, 2011 letter to defense counsel other than the fingerprint data that has already been produced.
4. Full and complete copies of all video recordings made inside the closet in the basement of MIT Building 16 including, but not limited to, recordings made on January 4 and 6, 2011.
5. All data, documents, and tangible things that constitute or are evidence of the eyewitness identification procedure mentioned in paragraph G of the government's August 12, 2011 letter to defense counsel.

When the data referred to in this order is computerized electronic data, transmissions, or communications, the government shall provide copies, or enable the defense to make copies, of the data in its native, bit-by-bit form, including all metadata, if the government has the data in its native format including all metadata. If the government does not have the data in its native form, including all metadata, it is to provide copies or enable the defense to make copies in the same computer searchable format of the data that is within in the possession, custody and control of the government, including optical

character recognition software format.

Any and all documents and information provided to Mr. Swartz, his counsel, his counsel's investigators and defense are to be used solely for the litigation of this case and no part of the documents or information may be disclosed or used for any other purpose.

SO ORDERED.

_____

JUDITH G. DEIN
United States Chief Magistrate Judge

Date:

Exhibit 2

U.S. Department of Justice

Carmen M. Ortiz
United States Attorney
District of Massachusetts

Main Reception: (617) 748-3100

United States Courthouse, Suite 9200
1 Courthouse Way
Boston, Massachusetts 02210

August 12, 2011

Mr. Andrew Good
Good and Cormier
83 Atlantic Avenue
Boston, MA 02110

Re: United States v. Aaron Swartz
Criminal No. 11-CR-10260

Dear Counsel:

Pursuant to Fed. R. Crim. P. 16 and Rules 116.1(C) and 116.2 of the Local Rules of the United States District Court for the District of Massachusetts, the government provides the following automatic discovery in the above-referenced case:

A. Rule 16 Materials

1. Statements of Defendant under Rule 16 (a)(1)(A) & (a)(1)(B)

a. Written Statements

The defendant's booking sheet and fingerprint card from the Cambridge Police Department are contained on enclosed Disk 5.

There are numerous relevant statements not made to government agents drafted by Defendant Swartz before the date of his arrest contained in electronic media, such as Twitter postings, websites and e-mail. These are equally available to the defendant. Those that the government intends to use in its case-in-chief are available for your review, as described in paragraph A(3) below.

Subject thereto, there are no relevant written statements of Defendant Swartz made

following his arrest in the possession, custody or control of the government, which are known to the attorney for the government.

b. Recorded Statements

The defendant made recorded statements at the time of his booking by Cambridge Police on January 6, 2011. A copy of his booking video is enclosed on Disk 7.

c. Grand Jury Testimony of the Defendant

Defendant Aaron Swartz did not testify before a grand jury in relation to this case.

d. Oral Statements to Then Known Government Agents

Defendant Aaron Swartz made oral statements at the time of the search of his apartment to individuals known to him at the time to be government agents. The only statements made by him then which the government believes at this time to be material are memorialized in the affidavit in support of the search warrant for his office at Harvard, a copy of which affidavit is enclosed on Disk 3.

2. Defendant's Prior Record under Rule 16 (a)(1)(D)

Enclosed on Disk 3 is a copy of the defendant's prior criminal record.

3. Documents and Tangible Objects under Rule 16(a)(1)(E)

All books, papers, documents and tangible items which are within the possession, custody or control of the government, and which are material to the preparation of the defendant's defense or are intended for use by the government as evidence in chief at the trial of this case, or were obtained from or belong to the defendant, may be inspected subject to a protective order by contacting the undersigned Assistant U.S. Attorney and making an appointment to view the same at a mutually convenient time.

Because many of these items contain potentially sensitive, confidential and proprietary communications, documents, and records obtained from JSTOR and MIT, including discussion of the victims' computer systems and security measures, we will need to arrange a protective order with you before inspection. Please review the enclosed draft agreement and let us know your thoughts.

4. Reports of Examinations and Tests under Rule 16 (a)(1)(F)

Enclosed you will find Disks 1, 2, 5 & 6 containing reports of examination of the following:

- Acer laptop computer recovered at MIT
- Western Digital hard drive recovered at MIT
- HP USB drive seized from the defendant at the time of his arrest
- Apple iMac computer seized at Harvard
- Western Digital hard drive seized at Harvard
- HTC G2 cell phone seized during the search of the defendant's residence
- Nokia 2320 cell phone seized during the search of the defendant's residence
- Sony Micro Vault seized during the search of the defendant's residence
- Four Samsung hard drives delivered to the Secret Service by Defendant Swartz and his counsel on June 7, 2011 (Please note that because of the number of files contained on Samsung model HD154UI hard drive, serial number S1Y6J1C2800332, it has not been practicable to date to make a complete file list in an Excel readable format, unlike the other drives.)
- A fingerprint analysis report from the Cambridge Police Department with respect to the Acer Laptop and Western Digital hard drive recovered at MIT
- A supplemental fingerprint analysis report with respect to these items

While not required by the rules, intermediate as well as final forensic reports where available are enclosed for many of the recovered and seized pieces of equipment on Disks 6 and 1, respectively.

B. Search Materials under Local Rule 116.1(C)(1)(b)

Search warrants were executed on multiple pieces of electronic equipment and at multiple locations. Copies of the search warrants, applications, affidavits, and returns have already been provided to you, but are further found on Disk 3.

Four Samsung Model HD154UI hard drives were examined following their consensual and unconditional delivery to the United States Secret Service on June 7, 2011. As an additional precaution, a warrant, enclosed on Disk 3, was also obtained.

C. Electronic Surveillance under Local Rule 116.1(C)(1)(c)

No oral, wire, or electronic communications of the defendant as defined in 18 U.S.C. § 2510 were intercepted relating to the charges in the indictment.

D. Consensual Interceptions under Local Rule 116.1(C)(1)(d)

There were no interceptions (as the term "intercept" is defined in 18 U.S.C. § 2510(4)) of wire, oral, or electronic communications relating to the charges contained in the indictment, made with the consent of one of the parties to the communication in which the defendant was intercepted or which the government intends to offer as evidence in its case-in-chief.

E. Video Recordings

On January 4, 2011 and January 6, 2011, Defendant Aaron Swartz was recorded entering a restricted wiring closet in the basement of MIT's Building 16. Copies of relevant portions of the recordings (where he is seen entering, in, or exiting the closet) are enclosed on Disk 4.

F. Unindicted Coconspirators under Local Rule 116.1(C)(1)(e)

There is no conspiracy count charged in the indictment.

G. Identifications under Local Rule 116.1(C)(1)(f)

Defendant Aaron Swartz was a subject of an investigative identification procedure used with a witness the government anticipates calling in its case-in-chief involving a photospread documented by MIT Police Detective Boulter. Relevant portions of the police report of Detective Boulter and a copy of the photospread used in the identification procedure are enclosed on Disk 3. In both instances, the name of the identifying MIT student has been redacted to protect the student's continuing right to privacy at this initial stage of the case. On page 2 of the Report of Photo Array, USAO-000007, the initials beside each of the enumerated items have been redacted for the same reason.

H. Exculpatory Evidence Under Local Rule 116.2(B)(1)

With respect to the government's obligation under Local Rule 116.2(B)(1) to produce "exculpatory evidence" as that term is defined in Local Rule 116.2(A), the government states as follows:

1. The government is unaware of any information that would tend directly to negate the defendant's guilt concerning any count in the indictment. However, the United States is aware of the following information that you may consider to be discoverable under Local Rule 116.2(B)(1)(a):

- Email exchanges between and among individuals at MIT and JSTOR as they sought to identify the individual responsible for massive downloads on the dates charged in the Indictment. While the defendant has admitted to being responsible for the downloads and produced one copy of most of what was downloaded on these dates, these e-mails reflect JSTOR's and MIT's initial difficulties in locating and identifying him in light of the furtive tactics he was employing. The email exchanges will be made available in accordance with paragraph (A)(3) above.

- Counsel for the government understands that a number of external connections were made and/or attempted to the Acer laptop between January 4, 2011 and January 6, 2011, including from a Linux server at MIT and from China. The Linux server was connected to a medical center at Harvard periodically during the same period. While government

counsel is unaware of any evidence that files from JSTOR were extracted by third parties through any of these connections, the connection logs will be made available to you in accordance with paragraph (A)(3) above.

- An analysis of one of the fingerprints on the Acer laptop purchased and used by the defendant cannot exclude his friend, Alec Resnick. The analysis is being produced for you; see paragraph (A)(4) above.

- While not a defense or material, one or more other people used or attempted to use scrapers to download JSTOR articles through MIT computers during the period of Defendant Swartz's illegal conduct. On the evening of November 29, 2010, the network security team at MIT was contacted and investigated journal spidering occurring on the site of the Institute of Electrical and Electronic Engineers. It was tracked to a group of shared computers on which anyone at MIT can host a virtual machine. It was determined that a virtual machine had been compromised. The user was notified that scripts placed on it were downloading journals from JSTOR, IEEE and APS. The machines were taken offline early the morning of November 30, 2010.

- The login screen on the Acer laptop when observed by Secret Service Agent Pickett on January 4, 2011 identified the user currently logged in as "Gene Host." A user name is different from a host name, and accordingly is similarly immaterial.

2. The government is unaware of any information that would cast doubt on the admissibility of evidence that the government anticipates offering in its case-in-chief and that could be subject to a motion to suppress or exclude.

3. Promises, rewards, or inducements have been given to witness Erin Quinn Norton. Copies of the letter agreement with her and order of immunity with respect to her grand jury testimony are enclosed on Disk 3.

4. The government is aware of one case-in-chief witness who has a criminal record.

Please be advised that one of the government's prospective trial witnesses was the subject of a charge in Somerville District Court in 1998 of being a minor in possession of alcohol and that the case was dismissed the following month upon payment of court costs. The government intends to make no further disclosures with respect to this matter, as the criminal charge could have no possible admissibility under either Fed.R.Crim.P. 609 or 608(b). If you believe you are entitled to additional information, including the identity of the prospective witness, please advise the undersigned, in which event the government will seek a protective order from the court to permit non-disclosure.

5. The government is aware of one case-in-chief witnesses who has a criminal case pending.

Please be advised that one of the government's prospective trial witnesses has pending state charges brought on July 7, 2009, involving the Abuse Prevention Act, Possession of Burglarious Tools, Criminal Harassment, and Breaking and Entering in the Daytime With Intent to Commit a felony. The events underlying the charges arise from the break-up of a personal relationship. The government has withheld the name of the witness and the others involved to protect their privacy, but will make them available along with the police reports in its possession subject to a protective order ensuring that the names, events and reports will not be disclosed publicly until the trial of this case, should the Court determine that a charge or information contained in the police reports is admissible for the purposes of cross-examination.

6. Based on the timeline as the government presently understands it from Officer Boulter's report described in paragraph G above and contained on Disk 3, no named percipient witnesses failed to make a positive identification of the defendant with respect to the crimes at issue. As reflected in the report, three students present when the Acer computer and Western Digital hard drive were recovered from Building 20 by law enforcement stated that they did not see anyone come in and place the computer there. However, as the timeline reflects, this was not a failed identification, but rather that they were not percipient witnesses to the event which had occurred earlier.

I. Other Matters

The government has preliminary analysis notes prepared at Carnegie Mellon of certain code and files contained on the Acer Laptop, as referenced on Page 2 of SA Michael Pickett's Forensic Cover Report contained on Disk 1. While these are not encompassed by Rule 16 (a)(1)(F) (formerly 16(a)(1)(D)), the government will make these available for review as described in section (A)(3), above, subject to the same procedures proscribed for preliminary transcripts in Local Rule 116.4 (B)(2).

Your involvement in the delivery of four hard drives containing documents, records and data obtained from JSTOR creates potential issues in this case under the Rules of Professional Conduct, as I am sure you are aware. To avoid the potential for those issues under Rule 3.7 in particular, we propose a stipulation from your client that the hard drives were from him, thus taking you out of the middle and rendering the origin an uncontested issue under the Rule. This stipulation would be without prejudice to all arguments on both sides as to the admissibility of the drives and their contents at any proceeding.

The government is aware of its continuing duty to disclose newly discovered additional evidence or material that is subject to discovery or inspection under Local Rules 116.1 and 116.2(B)(1) and Rule 16 of the Federal Rules of Criminal Procedure.

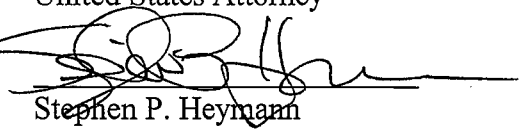
The government requests reciprocal discovery pursuant to Rule 16(b) of the Federal Rules of Criminal Procedure and Local Rule 116.1(D).

The government demands, pursuant to Rule 12.1 of the Federal Rules of Criminal Procedure, written notice of the defendant's intention to offer a defense of alibi. The time, date, and place at which the alleged offenses were committed is set forth in the indictment in this case a copy of which you previously have received.

Please call the undersigned Assistant U.S. Attorney at 617-748-3100 if you have any questions.

Very truly yours,

CARMEN M. ORTIZ
United States Attorney

By: 
Stephen P. Heymann
Scott L. Garland
Assistant U.S. Attorneys

enclosures